AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for securely providing information comprising the steps of:

(a) at a storage ~~sever~~ server, receiving from the client information identifying an encrypted personal security device;

(b) in response to receiving said information identifying a personal security device, sending from the storage server to the client said identified encrypted personal security device;

(c) at an authentication server, receiving authentication information from the client; and

(d) responsive to said authentication information, sending from a key server to the client decryption information for said personal security device.

2. (Canceled)

3. (Previously Presented) The method of claim 54, wherein the encrypted container contains information necessary to make a secure network connection between a network client and a network server.

4. (Previously Presented) The method of claim 54, wherein the encrypted container contains information necessary to make a secure virtual private network connection.

5. (Previously Presented) The method of claim 54, wherein authenticating involves validating said authentication information.

Claims 6-9 (Canceled)

10. (Previously Presented) The method of claim 54, wherein the received authentication information includes a time-based authentication code.

11. (Previously Presented) A method implemented by a client for accessing secure information comprising the steps of:

(a) receiving from a storage server an encrypted personal security device;

(b) receiving from a key server decryption information for said personal security device; and

(c) decrypting said personal security device.

12. (Canceled)

13. (Previously Presented) The method of claim 70, wherein the encrypted container contains information necessary to make a secure network connection between a network client and a network server.

14. (Previously Presented) The method of claim 70, wherein the encrypted container contains information necessary to make a secure virtual private network connection.

Claims 15 and 16 (Canceled)

17. (Previously Presented) The method of claim 70, wherein receiving the encrypted container involves receiving a smartcard that contains the encrypted container stored thereon.

18. (Previously Presented) The method of claim 70, further comprising storing the received key in a volatile memory.

Claims 19-51 (Canceled)

52. (Previously Presented) The method of claim 1, further comprising implementing the storage server and the authentication server on the same computer.

53. (Previously Presented) The method of claim 1, further comprising implementing the authentication server and the key server on the same computer.

54. (Currently Amended) A method for enabling a client to access secure information contained in an encrypted container, said method comprising:

at an authentication server, receiving from the client a key query that includes authentication information;

at the authentication server, authenticating the client based on the received authentication information; and

as a consequence of authenticating the client, sending a key from a key server to the client, said key for decrypting the ~~identified~~ encrypted container to access the secure information.

55. (Currently Amended) The method of claim 54, wherein the key query ~~identifyies~~ identifies the encrypted container.

56. (Previously Presented) The method of claim 54, further comprising:

at a storage sever, receiving from the client a request identifying the encrypted container containing secure information; and

in response to receiving said request, sending the identified encrypted container from the storage server to the client.

57. (Previously Presented) The method of claim 54, wherein authenticating the client involves:

in response to receiving the key query, sending the client an authentication challenge; and

receiving at the authentication server a response from the client to the authentication challenge, said response including said authentication information.

58. (Previously Presented) The method of claim 54, further comprising implementing the storage server and the authentication server on the same computer.

59. (Previously Presented) The method of claim 54, further comprising implementing the authentication server and the key server on the same computer.

60. (Currently Amended) The method of claim 54, wherein the encrypted container contains a ~~eryptrographic~~ cryptographic key.

61. (Previously Presented) The method of claim 54, wherein the encrypted container contains a password.

62 (Previously Presented) The method of claim 54, wherein the encrypted container contains private or secret information selected from a group consisting of a medical record,

contact information, a personal identification number, biometric information, a transaction record, and a map revealing a location of a resource.

63. (Previously Presented) The method of claim 54, wherein sending the key to the client involves transmitting the key through a connection to a computer network.

64. (Previously Presented) The method of claim 63, wherein the network connection is unencrypted.

65. (Previously Presented) The method of claim 63, wherein the network connection is encrypted.

66. (Previously Presented) The method of claim 63, wherein the computer network is the Internet.

67. (Previously Presented) The method of claim 54, wherein the received authentication information includes a single-use code.

68. (Previously Presented) The method of claim 54, wherein the received authentication information includes a event-based code.

69. (Previously Presented) The method of claim 54, wherein the received authentication information includes biometric information.

70. (Previously Presented) A method implemented by a client for accessing secure information, said method comprising:

receiving an encrypted container from a third party, said encrypted container containing the secure information;

sending a key request including authentication information to an authentication server;

in response to sending the authentication information to the authentication server, receiving from a key server a key for decrypting the encrypted container; and

with the received key, decrypting the encrypted container to access the secure information.

71. (Previously Presented) The method of claim 70, wherein said key request identifies the encrypted container.

72. (Previously Presented) The method of claim 70, further comprising sending information to a storage server identifying the encrypted container, and wherein receiving the encrypted container the third party involves receiving the identified encrypted container from the storage server.

73. (Previously Presented) The method of claim 70, wherein sending the key request and authentication information comprises, in response to sending the key request, receiving from the authentication server an authentication challenge and responding to the authentication challenge with the authentication information.

74. (Previously Presented) The method of claim 70, further comprising, after decrypting the encrypted container, completely erasing the received key from all client memory.

75. (Previously Presented) The method of claim 70, further comprising, after accessing the secure information, completely erasing the decrypted container and the secure information from all client memory.

76. (Currently Amended) The method of claim 70, wherein the encrypted container contains a ~~cryptrographic~~ cryptographic key.

77. (Previously Presented) The method of claim 70, wherein the encrypted container contains a password.

78. (Previously Presented) The method of claim 70, wherein receiving the key from the key server involves receiving the key through a connection to a computer network.

79. (Previously Presented) The method of claim 78, wherein the network connection is unencrypted.

80. (Previously Presented) The method of claim 78, wherein the network connection is encrypted.

81. (Previously Presented) The method of claim 78, wherein the computer network is the Internet.

82. (Previously Presented) The method of claim 70, further comprising generating a single-use code and wherein the authentication information comprises the single-use code.

83. (Previously Presented) The method of claim 70, further comprising generating a event-based code and wherein the authentication information comprises the event-based code.

84. (Previously Presented) The method of claim 70, further comprising generating biometric information and wherein the authentication information comprises the biometric information.

85. (Previously Presented) The method of claim 70, further comprising using an authentication token to generate the authentication information.

86. (Previously Presented) The method of claim 85, wherein the authentication token is a hardware device independent of the client.

87. (Previously Presented) The method of claim 85, wherein the authentication token is connected to the client.

88. (Previously Presented) The method of claim 85, wherein the authentication token is software running on the client.

89. (Previously Presented) The method of claim 85, wherein the authentication token is software running on a processor independent of the client.

90. (Previously Presented) The method of claim 70, wherein receiving the encrypted container involves receiving the encrypted container as an electronic communication over a network.